

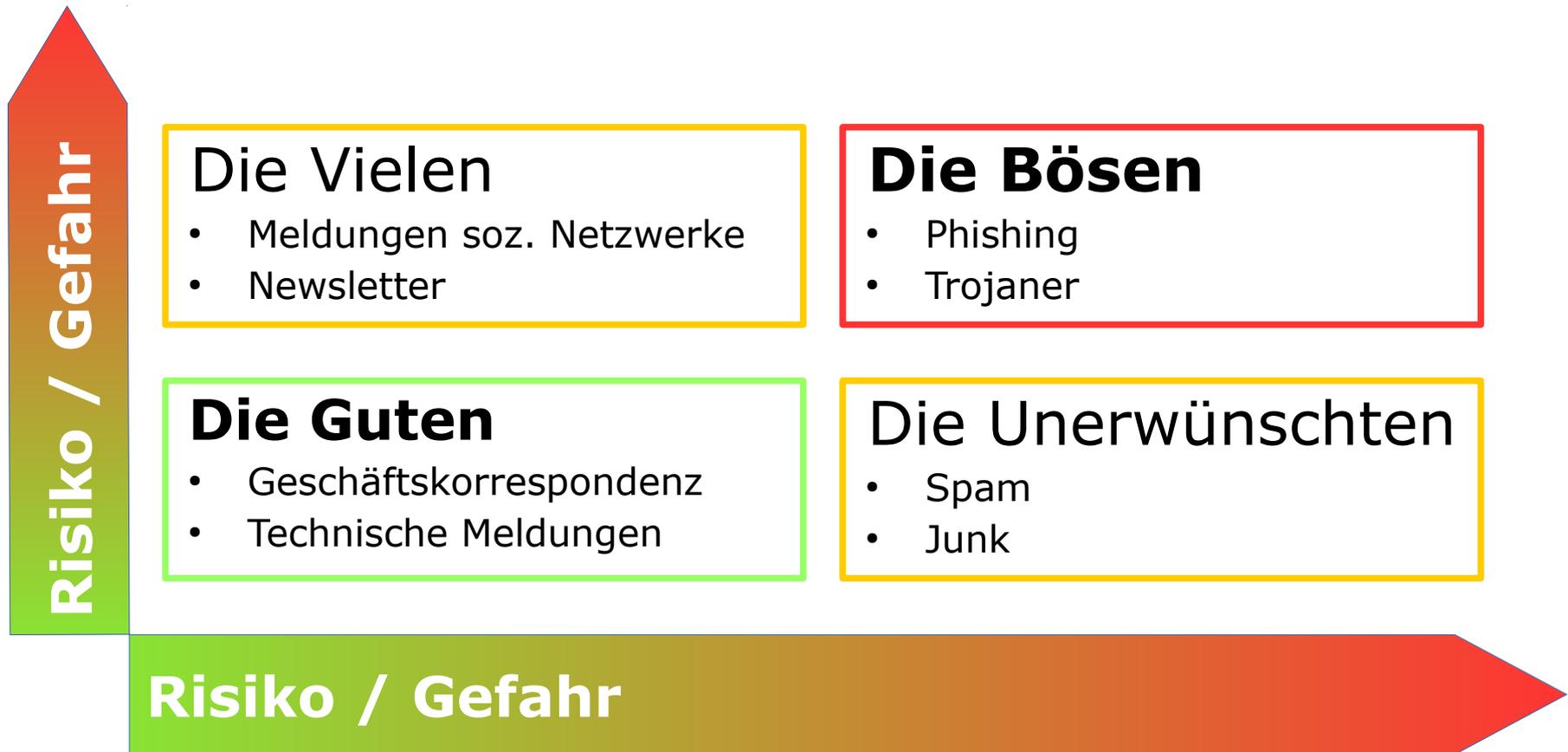
Gute Mails – böse Mails?

**Der sichere Umgang
mit E-Mails im Posteingang**

Agenda

- Gute Mails – Böse Mails
- Wer? Was? Und warum?
- Verhaltensregeln
- Werkzeuge zur E-Mail Analyse

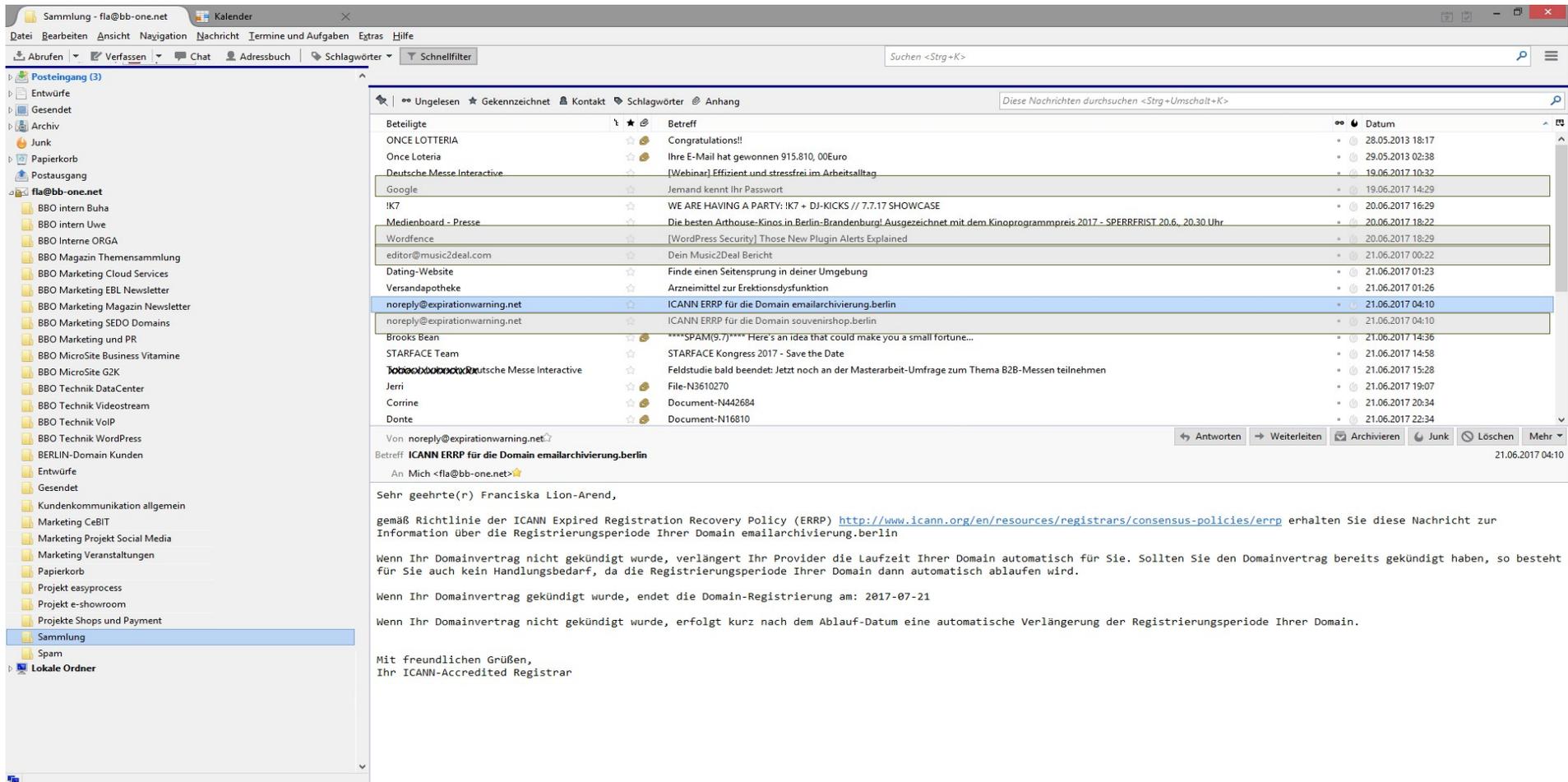
Gute Mails - Böse Mails



Wer? Was? Und warum?

- **Wer?**
 - Kriminelle
 - Geschäftemacher
- **Was?**
 - Spam / Junk
 - Phishing / Trojaner
- **Warum?**
 - Geld „verdienen“
 - Diebstahl, Erpressung & Betrug (Daten + Zugänge)
 - Terror

Beispiel 1: System-Meldungen



Beispiel 2: Newsletter-Einträge

Internetpartner der Wirtschaft

The screenshot shows an Outlook inbox with the following email list:

Beteiligte	Betreff	Datum
ONCE LOTTERIA	Congratulations!!	28.05.2013 18:17
Once Loteria	Ihre E-Mail hat gewonnen 915.810, 00Euro	29.05.2013 02:38
Deutsche Messe Interactive	[Webinar] Effizient und stressfrei im Arbeitsalltag	19.06.2017 10:32
Google	Jemand kennt Ihr Passwort	19.06.2017 14:29
IK7	WE ARE HAVING A PARTY: IK7 + DJ-KICKS // 7.7.17 SHOWCASE	20.06.2017 16:29
Medienboard - Presse	Die besten Arthouse-Kinos in Berlin-Brandenburg! Ausgezeichnet mit dem Kinoprogrammpreis 2017 - SPERRFRIST 20.6., 20.30 Uhr	20.06.2017 18:22
Wordfence	[WordPress Security] Those New Plugin Alerts Explained	20.06.2017 18:29
editor@music2deal.com	Dein Music2Deal Bericht	21.06.2017 00:22
Dating-Website	Finde einen Seitensprung in deiner Umgebung	21.06.2017 01:23
Versandapotheke	Arzneimittel zur Erektionsdysfunktion	21.06.2017 01:26
noreply@expirationwarning.net	ICANN ERRP für die Domain emailarchivierung.berlin	21.06.2017 04:10
noreply@expirationwarning.net	ICANN ERRP für die Domain souvenirshop.berlin	21.06.2017 04:10
Brooks Bean	****SPAM(9.7)**** Here's an idea that could make you a small fortune...	21.06.2017 14:36
STARFACE Team	STARFACE Kongress 2017 - Save the Date	21.06.2017 14:58
Deutsche Messe Interactive	Feldstudie bald beendet: Jetzt noch an der Masterarbeit-Umfrage zum Thema B2B-Messen teilnehmen	21.06.2017 15:28
Jerri	File-N3610270	21.06.2017 19:07
Corrine	Document-N442684	21.06.2017 20:34
Donte	Document-N16810	21.06.2017 22:34

The selected email is from Deutsche Messe Interactive with the subject "Feldstudie bald beendet: Jetzt noch an der Masterarbeit-Umfrage zum Thema B2B-Messen teilnehmen". The content of the email is as follows:

Von ~~XXXXXXXXXXXX~~ Deutsche Messe Interactive <~~XXXXXXXXXXXX~~@interactive.de>

Betreff: **Feldstudie bald beendet: Jetzt noch an der Masterarbeit-Umfrage zum Thema B2B-Messen teilnehmen**

An Mich <fla@bb-one.net>

Sehr geehrte Frau Lion-Arend,

anlässlich der dynamischen Entwicklungen im B2B-Messewesen führt Frau Lisa Knödler, Masterstudentin der Kommunikationswissenschaft an der Ostfalia Salzgitter, im Rahmen Ihrer Abschlussarbeit eine **Online-Befragung zum Thema „Bedeutung und Perspektive von B2B-Messen in Zeiten der Digitalisierung“** durch.

Selbstverständlich möchten wir Frau Knödler in Ihrem Vorhaben unterstützen. Ihr Unternehmen war bereits Messeaussteller oder plant dies? Dann wäre es von großer Bedeutung, wenn Sie sich ca. 10 Minuten Zeit für die Beantwortung der Fragen nehmen.

Da die **Umfrage in wenigen Tagen geschlossen wird**, bitten wir Sie, für eine hohe Datenqualität, **jetzt noch daran teilzunehmen**.

[>> Zur Umfrage](#)

Für Ihre Teilnahme und Unterstützung möchten wir uns bei Ihnen im Voraus bedanken!

Mit freundlichen Grüßen

Tobias Kozarsch

PS: Sie haben ein Netzwerk, das für diese Umfrage geeignet wäre? Gerne können Sie den Link weiterleiten und empfehlen. Jede Teilnahme steigert die Datengüte und damit die Qualität der Studie!

Beispiel 4: Betrugsversuch

Internetpartner der Wirtschaft

1. Von **XXXXXXXXXX@rbb-online.de** <hlwbraunau-office@eduhi.at>
2. Betreff: **Rech 53795112946 Franciska Lion-Arend**

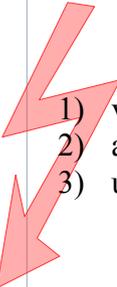
An: Info@imuse.tv
Datum: Mon, 26 Jun 2017 08:42:51 +0100
Nachrichten-ID: <54244964743.201762664251@imuse.tv>
Return-Path: <hlwbraunau-office@eduhi.at>
Received from EUR01-DBS-obe.outbound.protection.outlook.com

Guten Tag, Franciska Lion-Arend

siehe Anhang
Rech: <http://synchrnzr.com/Scan-00425482016/Franciska Lion-Arend>
Herzliche Grüße
XXXXXXXXXX@RBB-ONLINE.DE

3.

1.



- 1) vermeintlich seriöser Kontakt
- 2) abweichende Mailadresse
- 3) unseriöser, nicht passender Link

IP Address	3rd Party Info	Provider	City	Flag	Country
46.5.16.16	II II		Stuttgart	DE	Germany
104.47.2.219	II II		Dublin	IE	Ireland



Test-Tools FAILED!!

DOMAIN INFORMATION

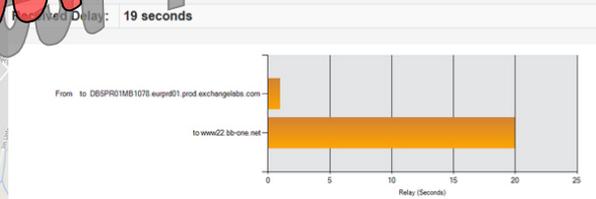
Domain: synchrnzr.com
Registrar: NETWORK SOLUTIONS, LLC.
Registration Date: 2004-05-04
Expiration Date: 2018-05-04
Updated Date: 2017-04-09
Status: clientTransferProhibited
Name Servers: dns1.nominalia.com, dns2.nominalia.com

REGISTRANT CONTACT

Name: FONT MORAGAS, DAVID
Street: Calle Doctor Letamendi 47 1-1
City: BARCELONA
Postal Code: 08031
Country: ES
Phone: +3492288411
Email: fontmoragas@synchrnzr.com

TECHNICAL CONTACT

Name: AMEN
Address: c/General Almirante 2-28, Barcelona, 08014, ES
Phone: +34 902888411, +34 914146171
Email: internic@amen.es



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	10.0.0.54	DBSPR01MB1078.eurprd01.prod.exchangelabs.com	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256)	6/26/2017 6:42:52 AM	✓
2	19 seconds	EUR01-DBS-obe.outbound.protection.outlook.com 104.47.2.219	ww22.bb-one.net	ESMTP	6/26/2017 6:43:11 AM	✗

Die wichtigsten drei Verhaltensregel

Regel Nummer EINS:

Anhalten, genau hinschauen und nachdenken!

- Kenne ich den Absender?
- Kann die Mailadresse stimmen?
- Habe ich einen bekannten Bezug zu Absender, Betreff oder Inhalt?
- Sind nicht verabredete Dateianhänge dabei?
- Werde ich aufgefordert, etwas zu tun?

Die wichtigsten drei Verhaltensregeln

Regel Nummer zwei:

**NICHTS öffnen,
was durch Regel 1 durchfällt!**

- unbekannte Absender mit merkwürdigen Namen und kryptischen Mailadressen
- vermeintlich bekannte Absender mit zweifelhaften Anfragen
- aktive Dateianhänge mit Endung .zip, .exe, .bat
- bearbeitbare Dateianhänge mit Endung .doc(x), .xls(x)", .ppt(x)

Die wichtigsten drei Verhaltensregeln

Regel Nummer drei:

LÖSCHEN! Denn per E-Mail...

- fragen Banken **niemals** nach Ihrem **Passwort** !
- **gewinnen / erben** Sie **niemals** irgend etwas !
- bekommen Sie keine **Rechnungen als .zip oder .doc**
→ **sondern als PDF !**

Weitere Maßnahmen

➤ **Datei-Anhänge**

- NIEMALS:
mit Doppelklick öffnen!
- Sondern:
 - rechte Maustaste
 - speichern &
kontrollieren
 - eventuell (!) öffnen

➤ **Absender überprüfen**

- per Telefon
- mit Werkzeug

Werkzeuge

- Bordmittel: E-Mail Client



- Domain-Abfrage

whois.nic.(TLD)

- www.mxtoolbox.com



- www.iptrackeronline.com

ipTRACKERonline.com
Geo-Information, IP-Adressen Tools und e-Whois for more

- www.network-tools.com



Weitere Links

- **Von den IT-Sicherheits-Profis:**
<https://www.sicherheitstest.bsi.de/>
- **Von der Verbraucherzentrale:**
<https://www.verbraucherzentrale.de/phishing-radar>
- **Aus Wissenschaft & Forschung:**
<https://www.cms.hu-berlin.de/de/dl/kommunikation/email/einfuehrung-e-mail>